UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,621	12/08/2003	Somnath Viswanath	H1226	4283

29393 7590 11/01/2007

ESCHWEILER & ASSOCIATES, LLC
NATIONAL CITY BANK BUILDING
629 EUCLID AVE., SUITE 1000
CLEVELAND, OH 44114

EXAMINER	
YALEW, FIKREMARIAM A	
ART UNIT	**PAPER NUMBER**
2136	

NOTIFICATION DATE	DELIVERY MODE
11/01/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing@eschweilerlaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/730,621	VISWANATH, SOMNATH	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-15 and 17-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-15 and 17-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The office action is in replay to an amendment filed on 03/12/2007. Claims 1,5,7-9,13 have been amended. Claims 4;16 are canceled. Claims 1-3,5-15,17-21 are pending.

2. The examiner withdraws the USC 112 rejection based on the applicant amendments.

Response to Arguments

3. Applicant's arguments with respect to claims 1-3,5-15,17-21 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-3,4-15,17-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Buer (US Pub no 20040128553) in view of Krishna et al (hereinafter referred as Krishna) WO 01/05086 A2 and further in view of Stanway, JR.et al (hereinafter referred as Stanway) US Pub No 20020129271 A1.

6. As per claim 1: Buer discloses a network interface system for interfacing a host system with a network to provide outgoing data from the host system to the network and to provide incoming data from the network to the host system, the network interface system comprising:

a bus interface system operable coupled with a host bus in the host system, the bus interface system being adapted to transfer data between the network interface system and the host system(See 0010 and Fig 1 steps 100,104);

a media access control system operable coupled with the network, the media access control system being adapted to transfer data between the network interface system and the network(See Fig 1 steps 112, and 0034,claim 28); a security system adapted to selectively encrypt outgoing data and to selectively decrypt incoming data from the network(See Fig 1 steps 122A,122D and 0034-0035,); and

a memory system, comprising first and second memories, the first memory being coupled with the media access control system and the security system and storing data from the network prior to security processing, the second memory being coupled to the security system and the bus interface system and storing data processed by the security system prior to transfer to the host system(See 0042,0060,0095);

wherein the security system comprises an input control system that controls data flow from the first memory into the security processing system, a core module that performs security processing on data received from the input control system, and an output control system that controls data flow from the security system to the second memory system(See 0032,0057);

However Buer does not explicitly disclose wherein the security system is configured to allow out-of-order writing of packet data to the output control system and the output control system assembles the out-of-order data in correct order within the second memory.

Krishna teaches wherein the security system is configured to allow out-of-order writing of packet data to the output control system and the output control system assembles the out-of-order data in correct order within the second memory (See page 3 lines 23-33, col 8 lines 20-29).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Buer and Krishna to include the security system is configured to allow out-of-order writing of packet data to the output control system and wherein the output control system assembles the out-of-order data in correct order within the second memory. This modification would have been motivated to do so, as suggested by (Krishna page 3 lines 26-27), inorder to provides a method for accelerating cryptography processing of data packets.

The combination of Buer and Krishna do not explicitly teach wherein the output control system is operable to receive at least a part of a decrypted payload of a subsequent packet before a status word of a preceding packet and the core module of the security system is operable to simultaneously decrypt and authenticate a packet payload.

However Stanaway teaches the output control system is operable to receive at least a part of a decrypted payload of a subsequent packet before a status word of a preceding packet (See 0019,0028) and the core module of the security system is operable to simultaneously decrypt and authenticate a packet payload (0006,0019,0028).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Buer to output control system is operable to receive at least a part of a decrypted payload of a subsequent packet before a status word of a preceding packet and the core module of the security system is operable to simultaneously decrypt and authenticate a packet payload. This modification would have been motivated to do so, inorder to improve the security of the system.

7. As per claim 2: the combinations of Buer-Krishna- Stanaway disclose wherein the bus interface system, the media access control system, the memory system, and the security system are included within a single integrated circuit. (See Buer 0148)

8. As per claim 3: the combinations of Buer-Krishna- Stanaway disclose wherein the input control system writes control words or status words associated with packets to be processed directly to the output control system, bypassing the core module (See Krishna col 2 lines 10-16).

9. As per claim 5: the combinations of Buer-Krishna- Stanaway disclose the network interface system wherein the output control system is operable to receive

control words for a packet while still waiting for part of a preceding packet (See Krishna col 9 lines 8-30).

10. As per claim 6: the combinations of Buer-Krishna- Stanaway disclose the network interface system wherein the part of the preceding packet comprises processed payload data within the core module (See Krishna col 9 lines 8-30).

11. As per claim 7: the combinations of Buer-Krishna- Stanaway disclose the network interface system wherein the output control system is operable to receive one or more status words for a packet after receiving part of a subsequent packet (See Krishna col 9 lines 23-28).

12. As per claim 8: the combinations of Buer-Krishna- Stanaway disclose the network interface system wherein the control module is operable to write decrypted data for a current packet prior to the second memory to writing a status word for a preceding packet thereto (See Buer Fig 8 steps 808, 810 and 0016-0017).

13. As per claim 9: the combinations of Buer-Krishna- Stanaway disclose the network interface system wherein the input control system is operable to selectively provide one copy of an initialization vector to the core module and another copy directly to the output control system (See Krishna col 9 lines 8-22).

14. As per clam 10: the combinations of Buer-Krishna- Stanaway disclose the network interface system wherein: the second memory is not word-addressable (See Krishna col 8 lines 20-29); the output control system comprises a word addressable buffer (See Krishna col 8 lines 20-29); and the output control system writes the contents of the word addressable buffer to the output buffer (See Krishna col 9 lines 10-22).

15. As per claim 11: the combinations of Buer-Krishna- Stanaway disclose the network interface system wherein the core module selectively authenticates packet using the HMAC-MD5-96 algorithm (See Buer 0133).

16. As per claim 12: the combinations of Buer-Krishna- Stanaway disclose the network interface system wherein the core module selectively authenticates packets using the HMAC-SHA-1-96 algorithm (See Buer 0133).

17. As per claim 13: Buer discloses a network interface system for interfacing a host system with a network to provide outgoing data from the host system to the network and to provide incoming data from the network to the host system, the network interface system comprising:

a bus interface system operable coupled with a host bus in the host system, the bus interface system being adapted to transfer data between the network interface system and the host system(See 0010 and Fig 1 steps 100,104);

a media access control system operable coupled with the network, the media access control system being adapted to transfer data between the network interface system and the network(See Fig 1 steps 122A,122D and 0034-0035);

a security system adapted to selectively decrypt and authenticate incoming data from the network(See Fig 1 steps 122A,122D and 0034-0035); and

a memory system, comprising first and second memories, the first memory being coupled with the media access control system and the security system and storing data from the network prior to security processing, the second memory being coupled to the

security system and the bus interface system and storing data processed by the security system prior to transfer to the host system(See 0042,0060,0095);

Buer does not explicitly disclose wherein the security system is configured to begin writing decrypted data for a subsequent packet to the second memory while completing authentication for a current packet.

However Krishna discloses wherein the security system is operable to begin writing decrypted data for a subsequent packet to the second memory while completing authentication for a current packet (See page 3 lines 23-33, col 8 lines 20-29)

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Buer to include the security system is configured to begin writing decrypted data for a subsequent packet to the second memory while completing authentication for a current packet. This modification would have been motivated to do so, as suggested by (Krishna page 3 lines 26-27), inorder to provides a method for accelerating cryptography processing of data packets.

The combination of Buer and Krishana do not explicitly teach a core module operable to decrypt completely the subsequent packet prior to authenticating the current packet.

However Stanaway teaches a core module operable to decrypt completely the subsequent packet prior to authenticating the current packet (See 0019,0028).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Buer and

kristhan to output control system is operable to receive at least a part of a decrypted payload of a subsequent packet before a status word of a preceding packet and the core module of the security system is operable to simultaneously decrypt and authenticate a packet payload. This modification would have been motivated to do so, inorder to improve the security of the system.

18. As per claim 14: the combinations of Buer-Krishna- Stanaway disclose the network interface system wherein the bus interface system, the media access control system, the memory system, and the security system are included within a single integrated circuit (See Buer 0148).

19. As per claim 15: the combinations of Buer-Krishna- Stanaway disclose the network interface system wherein the security system Contains pipelines for authentication and decryption that operate in parallel (See Krishna page 3 lines 23-33, col 8 lines 20-29).

20. As per claim 17: the combinations of Buer-Krishna-Stanaway disclose the network interface system wherein the core module authenticates the current packet using the HMAC-MD5-96 algorithm (See Krishna page 9 lines 1-7,col 11 line through col 12 line 17).

21. As per claim 18: the combinations of Buer-Krishna- Stanaway disclose the network interface system wherein the core module authenticates the current packet using the HMAC-SHA-1-96 algorithm (See Krishna page 9 lines 1-7, col 11 line through col 12 line 17)

22. As per claim 19: the combinations of Buer-Krishna- Stanaway disclose the network interface system wherein the security system comprises: an input control system; a core module coupled to the input control system (See Buer 0126-0130); and an output control system coupled to both the input control system and the core module, wherein the input control system is operable to receive a packet containing a control word data portion, a payload data portion, and a status word data portion, forward the control word data portion and the status word data portion directly to the output control system, and forward the payload data portion to the core module for decryption and authentication thereof(See Buer 0016,0032,0035).

23. As per claim 20: the combinations of Buer-Krishna- Stanaway the network interface system wherein the output controls system is operable to write decrypted data for the subsequent packet to the second memory concurrently with the core module completing authentication for the current packet (See Krishna page 3 lines 23-33, col 8 lines 20-29).

24. As per claim 21: the combinations of Buer-Krishna- Stanaway the network interface system wherein the output control system is operable to transmit the control word data portion, the payload data portion, and the status word data portion of packets to the second memory such that such packet portions are ordered in a predetermined fashion independent of an order such portions are received by the output control system (See Krishna page 3 lines 23-33, col 8 lines 20-29).

Conclusion

25. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew
18/14/2007
FA

Art Unit 2136
NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/18/07